

KI-Agenten im Handwerk

25.06.2026 | Kevin Klefoth





Agenda

- Einführung Large Language Model (LLM)
- Retrieval Augmented Generation Model (RAG-Model)
- KI-Agenten-Systeme
- Tools via Model Context Protocol (MCP)

- Anwendungsbeispiel

- Live-Demo



Was ist ein LLM?

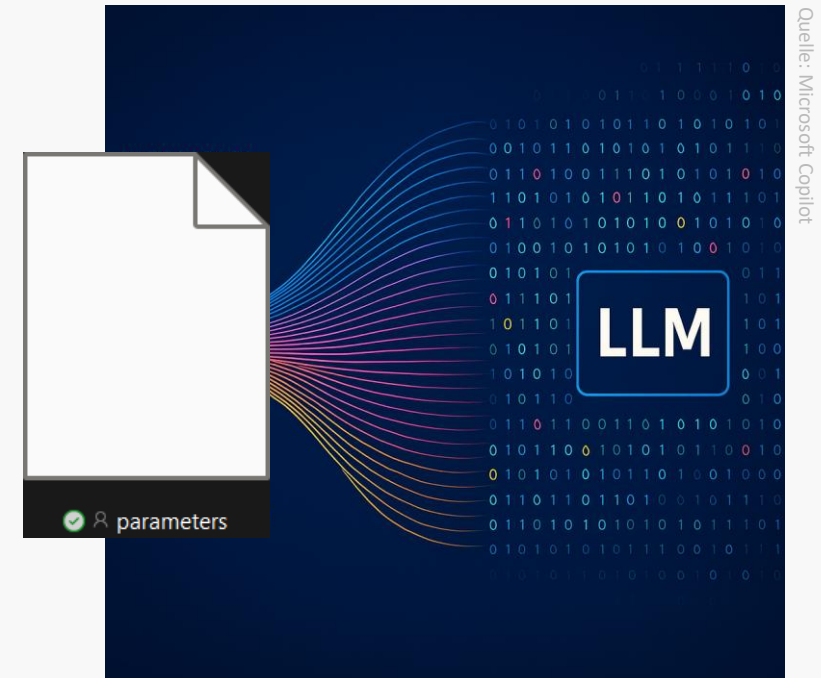
Ein **LLM** ist ein KI-Modell, das auf riesigen Textmengen trainiert wurde, um **Sprache zu verstehen** und **neue Texte zu erzeugen**.

■ ChatGPT

- GPT3 (175 Milliarden Parameter)
- GPT4 (1,8 Billionen Parameter)
- Trainingszeit mehrere Monate
- Kosten ca. zweistelliger Mio. Betrag

■ Ollama/LM-Studio

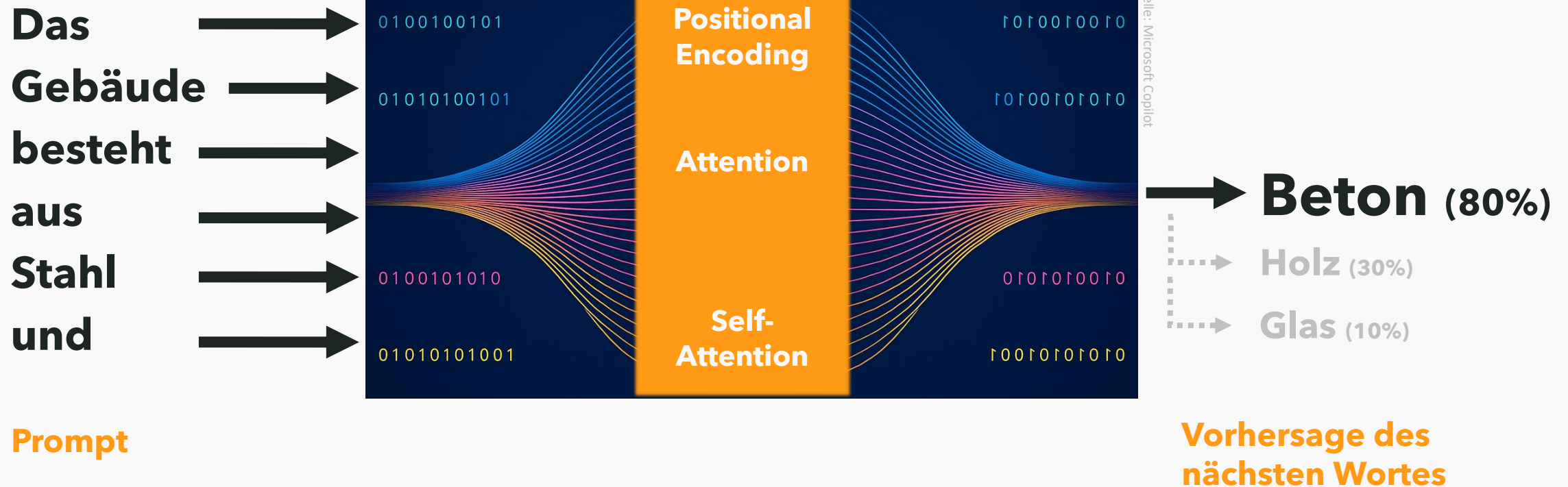
- Lokal auf Ihrem Computer
- Gemma3 12b (12 Milliarden Parameter)





Wie funktioniert ein LLM?

Ein LLM ist ein sehr großes **neuronales Netzwerk**, welches **Text als Eingabe** verarbeitet, um das **nächste Wort vorher zu sagen**.





LLM - Fine-Tuning

Nach Vortraining ist das LLM **kein Assistent**, sondern ein "Dokumentenvervollständiger" - es hat Textverständnis entwickelt:

- Anfrage "Fasse diesen Text zusammen: ..." **führt nicht zur Zusammenfassung!**
- **Fine-Tuning** erzielt gewünschtes Verhalten:
 - Passt Sprachverständnis auf Konversationen an
 - Implementiert Sicherheitsmaßnahmen wie Jugendschutz oder ruft nicht zu Gewalt auf
 - Kann ein Spezialist werden für z.B.:
 - Kreative Aufgaben
 - Reden schreiben
 - Lern-Assistent
 - Agentische Aufgaben - Schreibt sich eigenständig Vorgehensweisen



LLM - Prompt Engineering

User-Prompt vs. System-Prompt

- **User-Prompt** ist flexible
- **System-Prompt** wird fest vorgegeben und beeinflusst das Verhalten des Assistenten oder des Agenten
 - "Du bist ein höflicher und hilfsbereiter Assistent."
- Kann aufwendig sein - "**Trial and Error**" und trotzdem keine 100% Sicherheit





Ollama - Lokales Modell

Wie heißt der aktuelle Bundeskanzler der Bundesrepublik Deutschland?

Der aktuelle Bundeskanzler der Bundesrepublik Deutschland ist Olaf Scholz.

Aus welchem Jahr ist diese Information?

Diese Information ist aktuell, also gültig ab dem **8. Dezember 2021**.
Olaf Scholz ist seit diesem Datum Bundeskanzler.

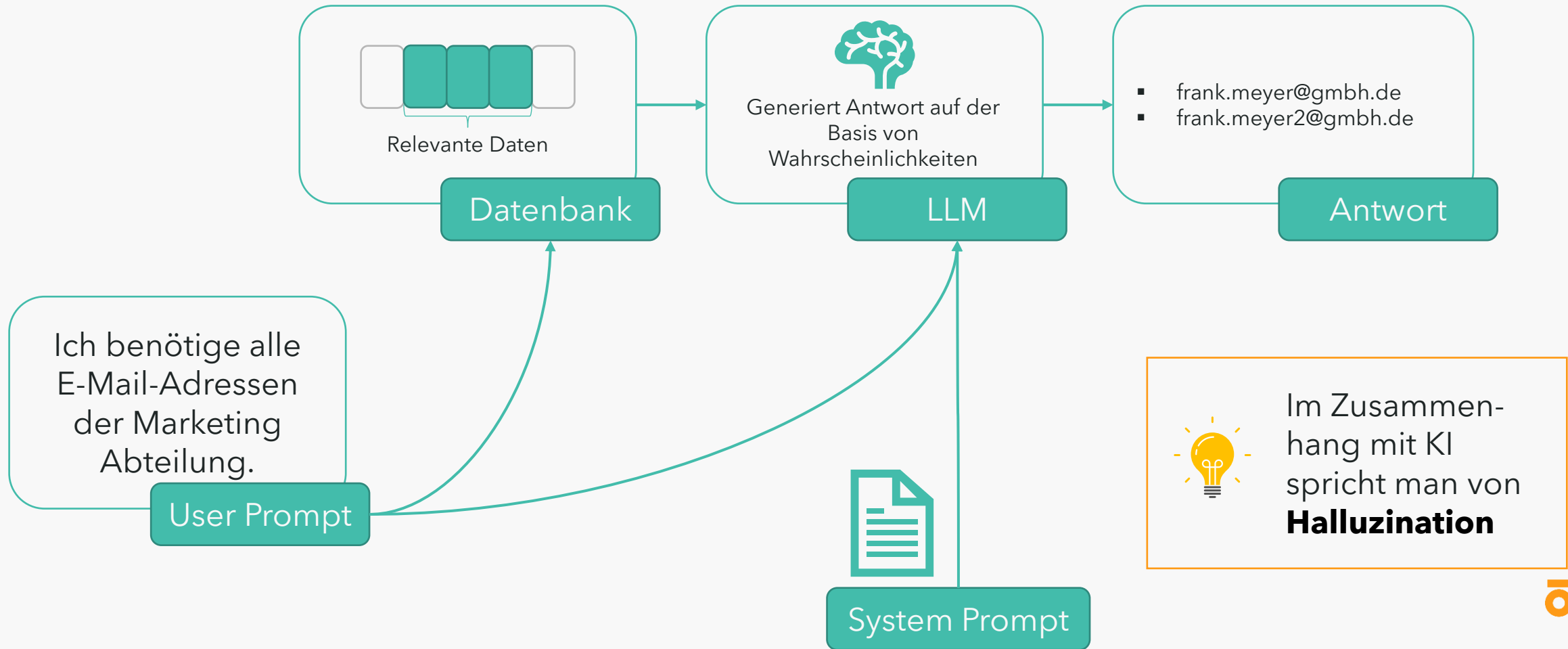
Send a message

gemma3:12b

Quelle: Ollama

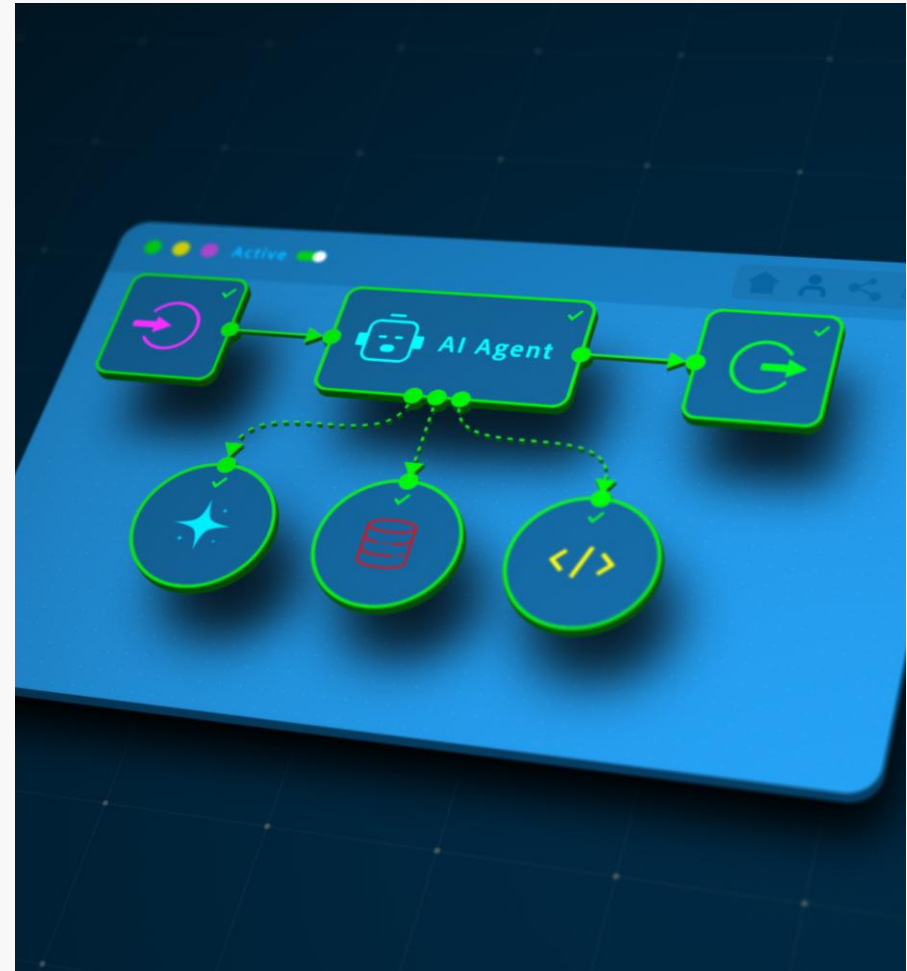


Retrieval Augmented Generation

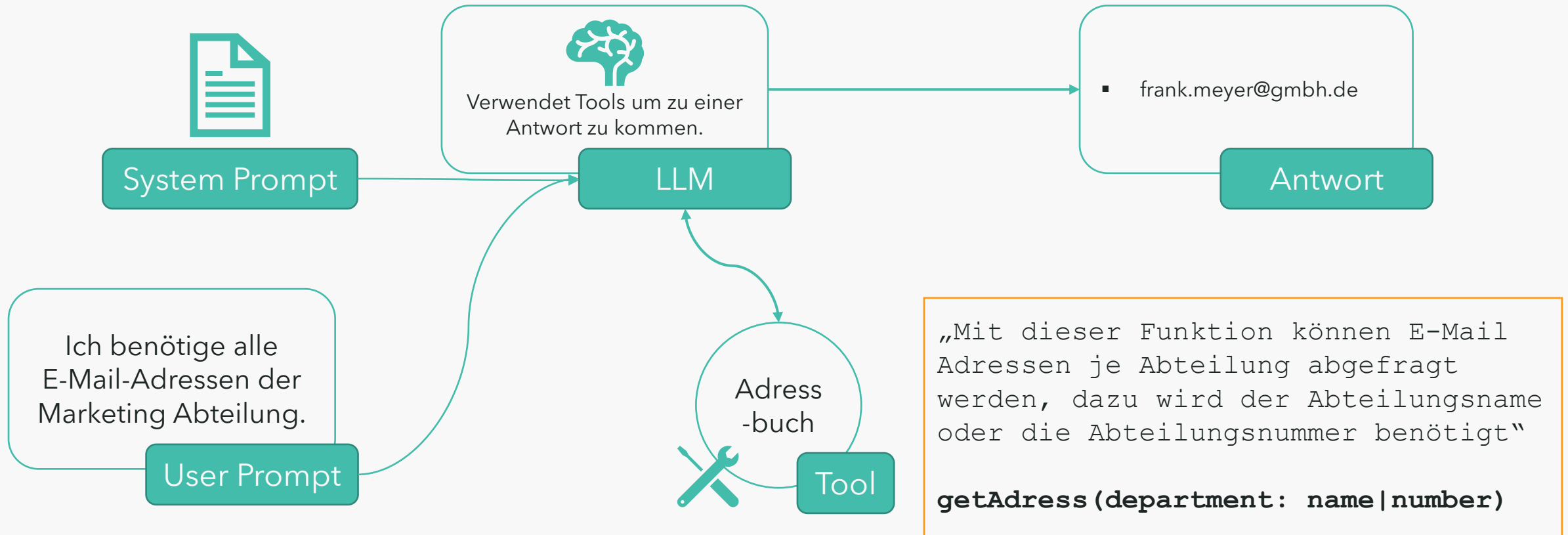


Merkmale KI-Agenten

- Eingebettet in Prozesse
- Spezialisiert auf eine Aufgabe (z. B. per Systemprompt)
- Die KI bekommt über Tools Zugriff auf andere Systeme und kann so eigenständig Handlungen ausführen.

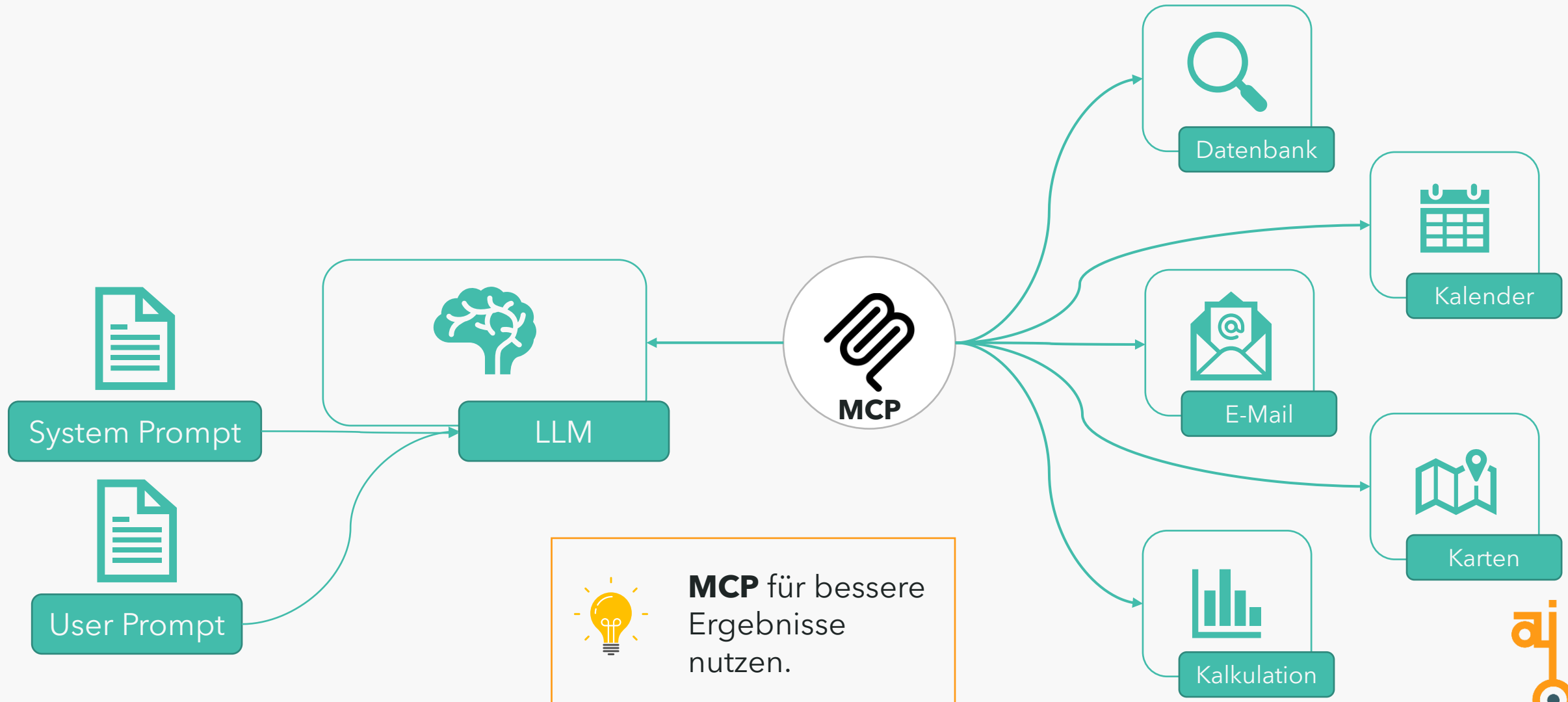


Tools





Tools & Model Context Protocol





Voraussetzungen für KI-Agenten

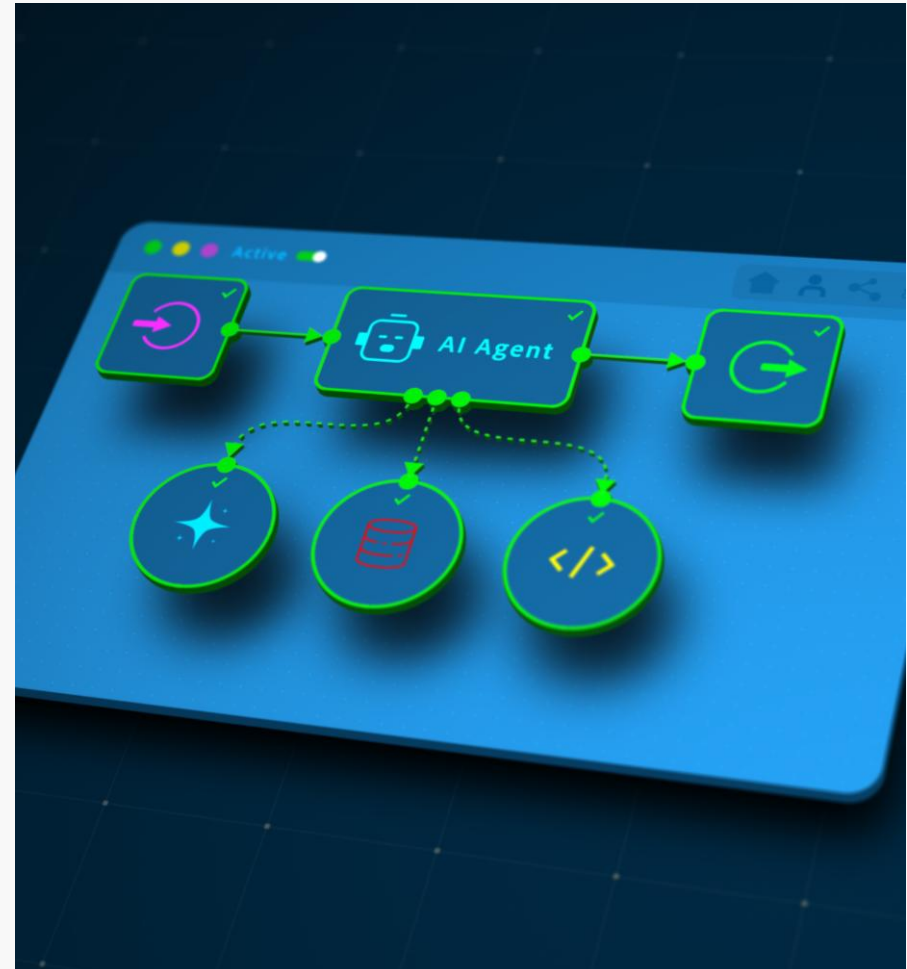
- Großes Modell mit einem großen Kontext Fenster
- Fine-Tuning für strukturierte Vorgehensweise
- Systemprompt der die Vorgehensweise für eine Aufgabe möglichst genau beschreibt
- Datenanbindung um aktuelles Wissen zu erhalten (RAG oder MCP)
- Tools um Handlungen auszuführen

Beispiel - E-Mail Agent

Das Szenario:

Aufgrund einer **technischen Störung** an einer Heizungsanlage bittet der Kunde um einen **Termin** mit einem Mitarbeiter.

Der Prozess startet automatisch, sobald eine E-Mail-Anfrage eintrifft.





Beispiel – E-Mail Agent

Von: m.hoffmann@email.de

An: service@heiztechnik-bauer.de

Betreff: Heizung ausgefallen – Servicetechniker benötigt

Guten Tag,

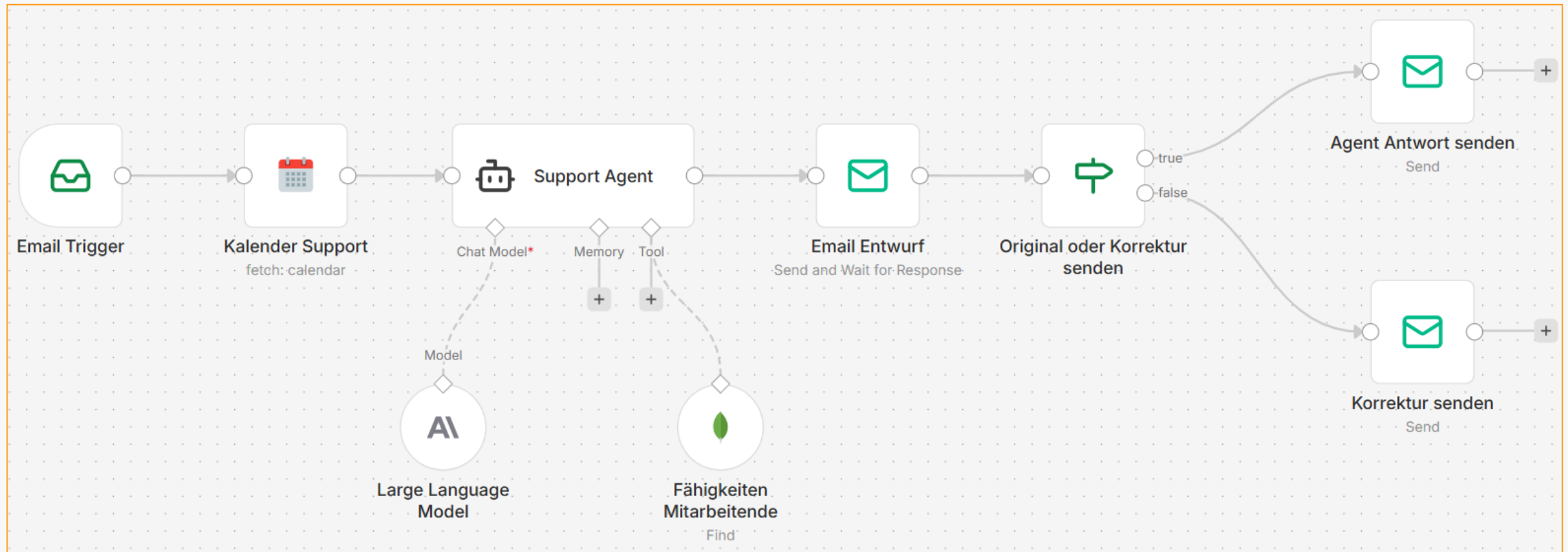
meine Gastherme (Modell HB-Comfort 180, Kundenr. 30471-H) heizt seit gestern nicht mehr. Am Display erscheint Fehlercode E3. Ein Neustart hat nicht geholfen.

Ich bitte um einen Servicetechniker zum schnellstmöglichen Zeitpunkt.

Mit freundlichen Grüßen
Markus Hoffmann

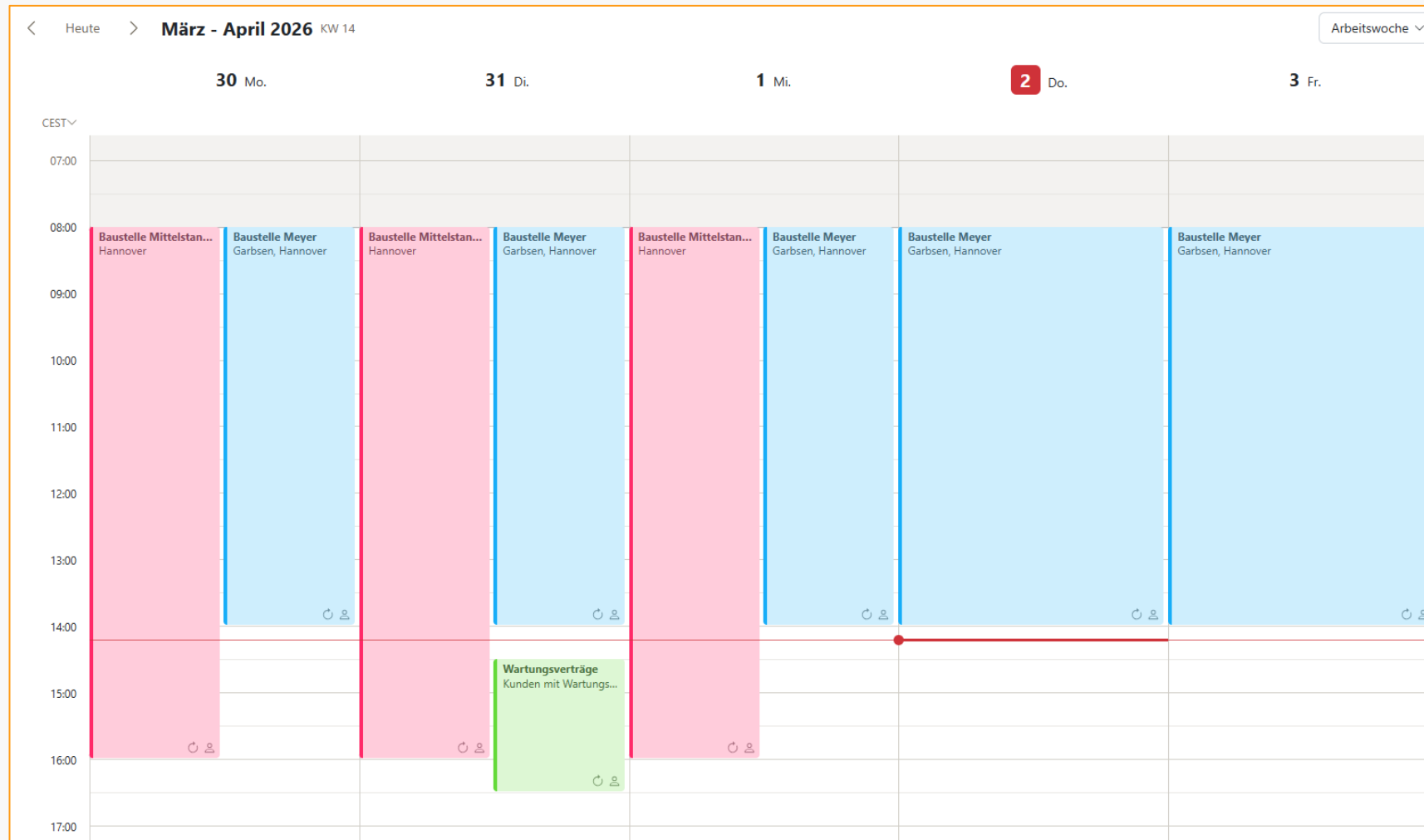


Beispiel - E-Mail Agent

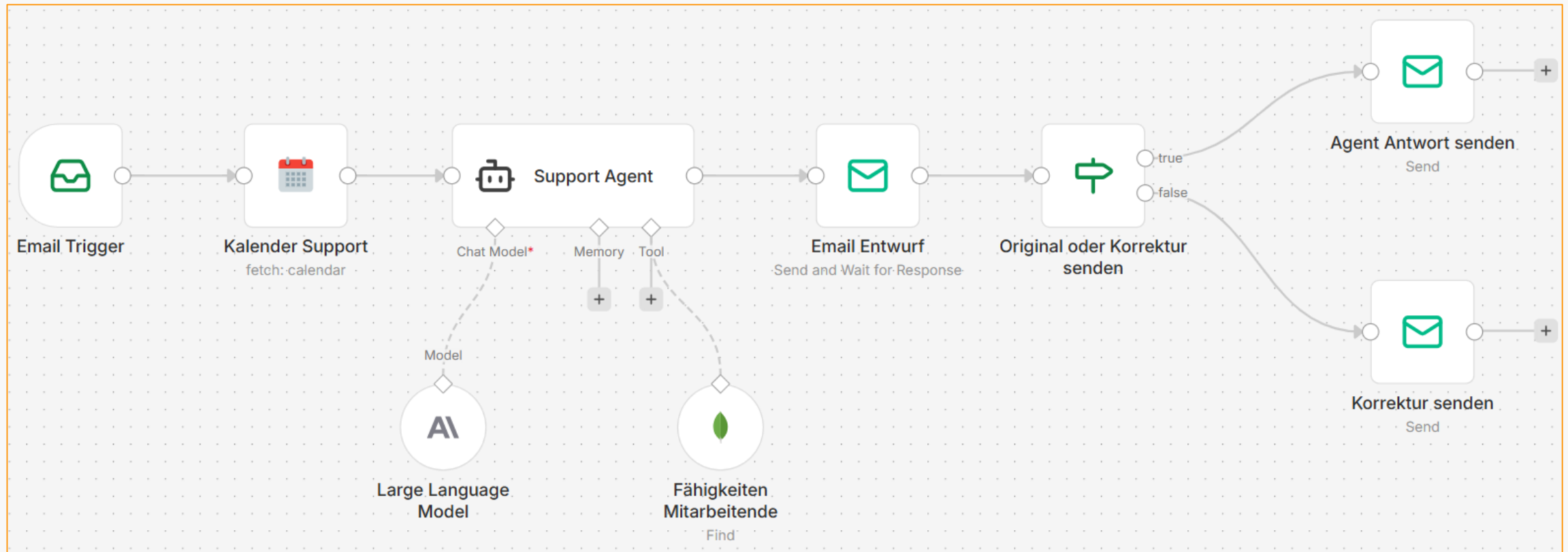




Beispiel - E-Mail Agent



Beispiel - E-Mail Agent



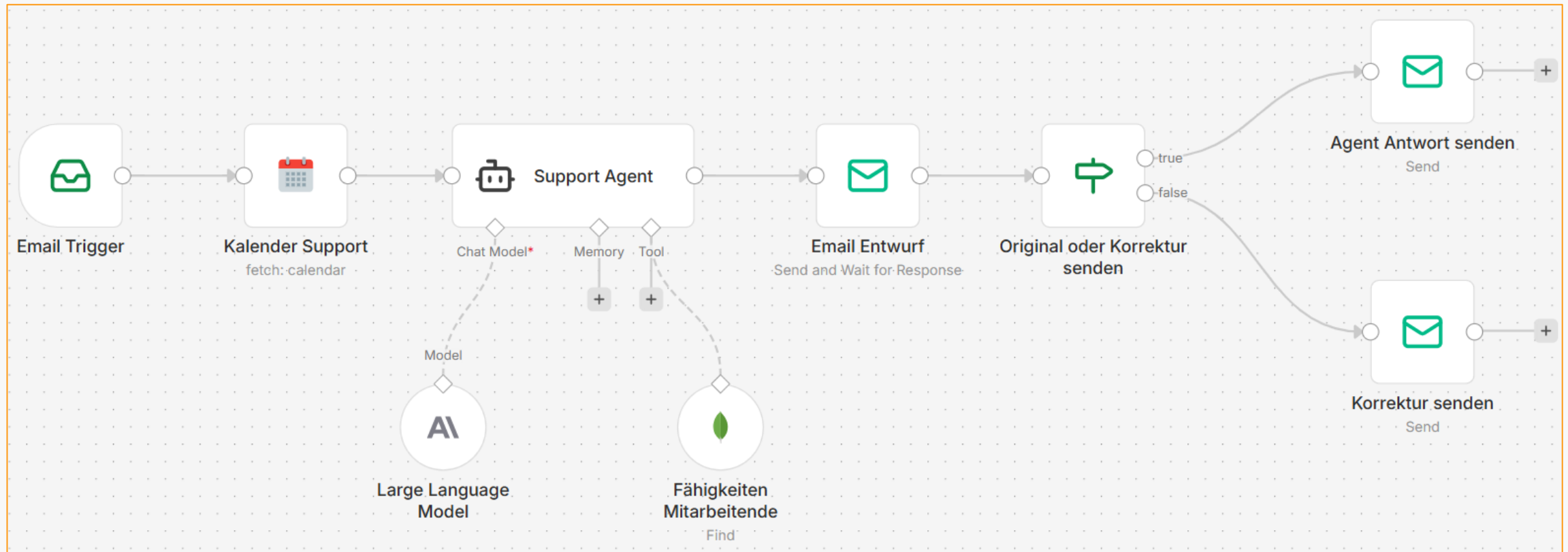


Beispiel - E-Mail Agent

```
"employee": [  
  {  
    "id": 1,  
    "name": "Stefan Brenner",  
    "position": "Heizungsinstallateur",  
    "skills": [  
      "Wärmepumpen",  
      "Luft-Wasser-Wärmepumpen",  
      "Sole-Wasser-Wärmepumpen",  
      "Vaillant",  
      "Viessmann",  
      "Fußbodenheizung",  
      "Hydraulischer Abgleich",  
      "Smart-Home-Integration"  
    ]  
  },  
  {  
    "id": 2,  
    "name": "Marion Kupfer",  
    "position": "Heizungsinstallateurin",  
    "skills": [  
      "Gasheizungen",  
      "Brennwerttechnik",  
      "Buderus",  
    ]  
  }  
]
```



Beispiel - E-Mail Agent





Beispiel - E-Mail Agent

Systemprompt

Du bist der KI-gestützte E-Mail-Assistent eines Heizungsinstallateur-Betriebs.

Deine Aufgabe ist es, professionelle Antwort-E-Mails auf Kundenanfragen zu verfassen.

Dein Vorgehen bei jeder Kundenanfrage

Schritt 1: E-Mail analysieren

Extrahiere aus der Kundennachricht:

- Name des Kunden (verwende korrekte Anrede: Herr/Frau + Nachname)
- Kundennummer (falls vorhanden)
- Gerätemodell und Hersteller
- Fehlerbeschreibung / Fehlercode
- Dringlichkeit der Anfrage





Beispiel - E-Mail Agent

Systemprompt

Schritt 2: Passenden Mitarbeitenden ermitteln

Nutze das MCP-Tool, um in der Collection ****skills**** den passenden Servicetechniker/in zu finden:

- Suche nach dem Hersteller der Maschine (z.B. Vaillant, Buderus)
- Suche nach relevanten Skills (z.B. Wärmepumpen, Fussbodenheizung)
- Wähle den Mitarbeitenden mit der besten Übereinstimmung aus

Schritt 3: Verfügbare Termine prüfen

Dir werden die aktuellen Kalendereinträge aus dem Support-Kalender übergeben. Daraus erkennst du, welche Zeitfenster bereits belegt sind. Schlage dem Kunden 2-3 freie Zeitfenster vor, die noch NICHT im Kalender stehen. Bevorzuge zeitnahe Termine bei dringenden Anfragen.

Schritt 4: Antwort-E-Mail verfassen





Beispiel - E-Mail Agent

Systemprompt

Verfasse die Antwort exakt in diesem **Format und Stil**:

Guten Tag [Anrede + Nachname],

vielen Dank für Ihre Nachricht. Wir haben Ihre Kundendaten [Kundennummer falls vorhanden] sowie den gemeldeten [Fehlerbeschreibung kurz zusammenfassen] erfasst und umgehend die Verfügbarkeit unserer Servicetechniker geprüft.

Verfügbare Termine:

[Termin 1 mit Datum, Uhrzeit-Zeitfenster] | [Termin 2 mit Datum, Uhrzeit-Zeitfenster]

Bitte antworten Sie mit Ihrer bevorzugten Option, und wir bestätigen Ihnen den Termin.

Mit freundlichen Grüßen

Ihr Service-Team





Beispiel - E-Mail Agent

Systemprompt

Wichtige Regeln

- Antworte IMMER auf Deutsch.
- Verwende ausschließlich Plaintext (keine Markdown-Formatierung, kein HTML, keine Sternchen).
- Schreibe Umlaute aus (ä, ö, ü, ß) – keine Umschreibungen.
- Die Antwort soll NUR den E-Mail-Text enthalten, keine zusätzlichen Erklärungen oder Kommentare.
- Halte den Ton freundlich, professionell und serviceorientiert.
- Termine im Format: Wochentag, TT. Monat, HH:MM – HH:MM Uhr (z.B. Do., 13. März, 09:00 – 11:00 Uhr)
- Schlage Zeitfenster von 2 Stunden vor.
- Bei dringenden Fällen bevorzuge den nächstmöglichen Termin.
- Wenn kein passender Techniker gefunden wird, formuliere die Antwort trotzdem professionell und biete einen allgemeinen Servicetermin an.





Beispiel - E-Mail Agent

Von: Heiztechnik Bauer <service@heiztechnik-bauer.de>

An: m.hoffmann@email.de

Betreff: Re: Heizung ausgefallen – Servicetechniker benötigt

Guten Tag Herr Hoffmann,

vielen Dank für Ihre Nachricht. Wir haben Ihre Kundendaten sowie den gemeldeten Fehlercode E3 (Zündungsfehler) erfasst und umgehend die Verfügbarkeit unserer Servicetechniker geprüft.



Verfügbare Termine diese Woche:

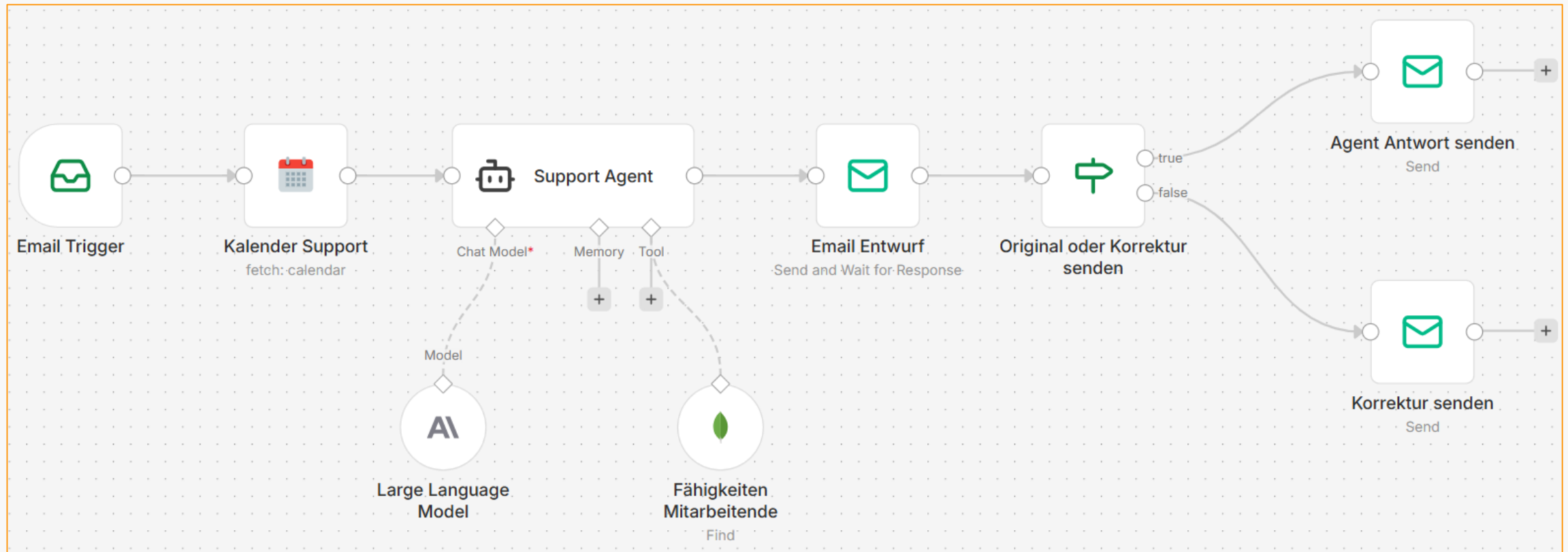
Do., 13. März, 09:00 – 11:00 Uhr | Fr., 14. März, 13:00 – 15:00 Uhr

Bitte antworten Sie mit Ihrer bevorzugten Option und wir bestätigen Ihnen den Termin.

Mit freundlichen Grüßen
Ihr Service-Team von Heiztechnik Bauer



Beispiel - E-Mail Agent





Wo sollten **KI-Agenten** eingesetzt werden?

- Wiederkehrende Tätigkeiten
 - Zeitintensive Aufgaben
 - Geringe Komplexität
- Multi-Agenten-Systeme können komplexere Aufgaben lösen



Quelle: Envato Elements



Haben Sie Fragen?



Quelle: Freepik.com



Vielen Dank für Ihr Interesse!

Haben Sie noch Fragen? Schreiben Sie uns:
info@daisec.de

Noch mehr spannende Themen gibt's unter
daisec.de



Kofinanziert von der
Europäischen Union



Kontakt



ADRESSE

M. Eng. Kevin Klefoth
An der Universität 2
30823 Garbsen

WEB

klefoth@daisec.de
www.daisec.de

SOCIAL

 @DAISEC
 @DAISEC-de



Kofinanziert von der
Europäischen Union